OFICIÁLNÍ DEKLARACE SOULADU S GDPR

Nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a jeho implementace

Nařízení 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Společnost TRUE TRAC s.r.o. si je plně vědoma významu ochrany osobních, provozních a lokalizačních údajů, a proto při shromažďování a dalším zpracování takových údajů, včetně obsahu, postupujeme v souladu s platnými právními předpisy, zejména se zákonem č.101/2000 Sb., o ochraně osobních údajů, se zákonem č.127/2005 Sb., o elektronických komunikacích, podle Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES a dále dle příslušných ustanovení Občanského zákoníku, jakož i příslušných norem Evropské unie.

Nejenže aktivně sledujeme vývoj české legislativy a legislativy EU, abychom implementovali veškeré požadavky uložené zákonem, ale aktivně se věnuje oblasti ochrany dat a bezpečnosti – například tím, že máme definovanou a funkční roli **Data Privacy Officera (DPO)**.

Můžeme deklarovat, že splňujeme požadavky platných právních předpisů v oblasti ochrany osobních údajů a že implementujeme požadavky **nařízení 2016/679** o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „**GDPR**“), a tedy ode dne aplikovatelnosti jsme připraveni na plnění povinností kladených GDPR jak na správce osobních údajů, tak na případy, kde bude společnost TRUE TRAC s.r.o. v pozici zpracovatele osobních údajů.

Jsme držitelem **certifikátu** podle normy **ČSN ISO/IEC 27001:2013**, který prokazuje, že naše společnost přijala všechna nezbytná opatření k ochraně citlivých informací (jimiž se zejména rozumí nejen osobní údaje, ale i zákaznické údaje jako celek) před neoprávněným přístupem, sladila interní postupy s požadavky normy a plní legislativní a jiné požadavky. I tak, a to zejména s ohledem na možné nové bezpečnostní hrozby, jsou bezpečnostní opatření neustále posuzována ve světle konkrétních okolností, aby se určila a zabezpečila vhodná úroveň ochrany.

Povinnost vést záznamy o činnostech zpracování

Ode dne aplikovatelnosti GDPR, tedy od 25. 5. 2018, jsou nastaveny veškeré procesy nezbytné k vedení záznamů v rozsahu požadovaném GDPR, a to jak na případy, kdy je společnost TRUE TRAC s.r.o. v pozici správce, tak na případy, kdy je společnost TRUE TRAC s.r.o. v pozici zpracovatele. Již dnes dokumentujeme veškeré činnosti zpracování, které jsou podle současné platné právní úpravy předmětem registrace u Úřadu pro ochranu osobních údajů.

Posouzení vlivu na ochranu osobních údajů

Řízení rizik je jednou z klíčových oblastí, která je již dnes v naší společnosti plně implementována v rámci systému řízení bezpečnosti informací, jejíž jsou osobní údaje součástí, zejména řízení rizik a zajištění souladu s právní úpravou. Máme nastaveny procesy, v rámci nichž budou implementovány požadavky GDPR tak, aby zejména při využití nových technologií a s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, které by mohlo mít za následek vysoké riziko pro práva a svobody fyzických osob, bylo předem provedeno posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.

Ohlašování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a Oznamování případu porušení zabezpečení osobních údajů subjektu údajů

V rámci incident managementu máme nastaveny procesy pro řádné dokumentování veškerých bezpečnostních incidentů a pro ohlašování porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a oznamování

subjektu údajů. Jako poskytovatel služeb GPS monitoringu jsme již dnes povinni oznámit Úřadu pro ochranu osobních údajů porušení ochrany osobních údajů, ke kterému by došlo v rámci poskytované služby GPS monitoringu.

Ustavení pověřence pro ochranu osobních údajů

Máme ustanoveného Pověřence pro ochranu osobních údajů (DPO), který je vybaven odpovídajícími pravomocemi a je zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.

Data Privacy Officer (DPO)

Miroslav Černý

+420 603 251 159

cerny@czech-gss.cz

Práva subjektu údajů

Veškeré povinnosti kladené na společnost TRUE TRAC s.r.o. jako správce ve vztahu k právům subjektu údajů byly ke dni aplikovatelnosti GDPR splněny. Zároveň začala naše společnost zajišťovat veškerou součinnost správcům nutnou k plnění jejich zákonných povinností podle GDPR, jimž poskytujeme služby v pozici zpracovatele.

V rámci projektu implementace GDPR byly nastaveny pro každý subjekt údajů, který je pro naši společnost identifikovaný nebo identifikovatelný, takové postupy, aby subjekt údajů měl jednoduše dostupné veškeré informace nově požadované GDPR a aby mohl jednoduchým způsobem uplatňovat svá nová práva, která pro něj z GDPR vyplývají.

Technické postupy a opatření k zajištění bezpečnosti osobních údajů

K dosažení všech požadavků kladených GDPR byla v systému doimplentována a přijata řada technických opatření, aby nedošlo k narušení zpracovávaných údajů. Chránit osobní údaje je nutné ze dvou pohledů:

- proti poškození, ztrátě, neoprávněnému přístupu uložených osobních údajů
- proti odposlechu a pozměňování osobních údajů při přenášení dat po síti

Autentizace

Autentizace znamená ověření prohlašované identity subjektu. Metody takového ověření jsou typicky založené na něčem, co uživatel zná (typicky přihlašovací jméno a heslo). V našem systému je použita metoda kombinace hesla a jednorázového hesla. Jednorázové heslo (anglicky One-time password, zkratka OTP) je heslo, které je platné pouze pro jedno přihlášení nebo pro jednu transakci. Speciální subsystém heslo generované serverem odesílá uživateli na nezávislém kanálu v podobě emailu, sms nebo telegramové zprávy. Generování hesel je založeno na derivaci Lamportova schématu.

Autorizace

Jedná se o proces následující po autentizaci. Autorizace je proces určování, zda může subjekt provádět určité operace. V našem systému je použita víceurovňová metoda přiřazování pohledů a akcí nad konkrétními kategoriemi osobních údajů, popřípadě granularity přístupu na konkrétní objekty.

Bezpečnost

V systému je zajištěna kontrola přístupu na různých úrovních. Přístup je rozdělen podle dostupných operací nad konkrétními typy dat. Kontrola přístupu může být nastavena v závislosti na různých vlastnostech dat. Například na obsahu, kontextu (čas, místo), historii (sekvence dotazů) či výsledku kontrolních procedur, které se provádějí v době použití. Systém podporuje průběžné změny oprávnění uživatelů v závislosti na úlohách, které právě provádějí. Požadavek na víceúrovňovou ochranu je determinován citlivým prostředím zpracovávání zvláštních osobních údajů (sledování geografické polohy subjektů). V systému je prováděna oddělením interního auditu pravidelná kontrola inference, hlavně na agregaci a asociaci dat. Tuto kontrolu provádíme z nutnosti ošetření větší citlivosti agregovaných dat oproti jednotlivým položkám a také zabránění zjištění citlivých informací pomocí vztahů k neklasifikovaným datům.

Jednou z možností zajištění kontroly inference je násobnost výskytu. Data se v systému vyskytují několikrát, pokaždé s jinou bezpečnostní klasifikací. V systému je implementována podpora interního auditu (všechny akce týkající se bezpečnosti jsou strukturovaně zaznamenávány) a kontrola toků (kontrola cíle výstupních dat, jež byly získány oprávněným přístupem).

Pseudonymizace

Pseudonymizace osobních údajů je proces skrytí identity, jehož účelem je odbourání vazby mezi zpracovávanými osobními údaji a konkrétním subjektem údajů bez použití dodatečných informací.

V našem systému je pseudonymizace dosaženo odděleným uchováváním dodatečných informací, které vedou k přiřazení údajů konkrétnímu subjektu. Na tyto informace se vztahují technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.

Monitoring využití pseudonymizace provádí oddělení interního auditu pravidelnými bezpečnostními prověrkami.

Automatický výmaz dat

V systému si zákazník sám určí dobu dle svého Spisového řádu, po kterou jsou nashromážděná a zpracovávaná data v systému uchována. Toto nastavení se provádí zvlášť pro obě kategorie osobních údajů - osobní údaje a zvláštní osobní údaje. Údaje jsou po nastavené době ze systému automaticky nenávratně odstraněny, včetně odstranění ze všech zálohových a pasivních subsystémů.

Certifikáty